COMBINED ARMS IN THE ELECTRO-MAGNETIC SPECTRUM: INTEGRATING NON-KINETIC OPERATIONS

A Monograph

by

Major Jeffrey C. Crivellaro
USAF

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-05-2013	Monograph	June 2012 - May 2013

4. TITLE AND SUBTITLE
Combined Arms in the Electromagnetic Spectrum: Integrating Non-Kinetic Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Crivellaro, Jeffrey, C.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
1 Reynolds Avenue
Fort Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC, SAMS

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Anti-access, area denial (A2AD) environments provide adversaries with an asymmetric advantage too costly for a 21st - century military to overcome. Arguably, a counter to a defense-in-depth environment is an attack-in-depth strategy. However, regaining a relative advantage requires leveraging the electro-magnetic spectrum to offset the high cost of traditional targeting methodologies. This monograph suggests a framework for negating an anti-access, area denial advantage by integrating non-kinetic operations to induce strategic paralysis within the enemy's decision cycle. Electronic warfare, computer network operations, and space control negation require the same level of command and control, integration, and synchronization as kinetic fires in order to produce discernible effects on the battlespace.

15. SUBJECT TERMS
Non-kinetic operations (NKO), computer network operations (CNO), electronic warfare (EW), cyber warfare, electromagnetic spectrum (EMS) control, air operations center (AOC), operational art, computer security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	(UU)	43	COL Thomas C. Graves
(U)	(U)	(U)			19b. TELEPONE NUMBER (*Include area code)* 913-758-3300

MONOGRAPH APPROVAL PAGE

Name of Candidate: Major Jeffrey C. Crivellaro

Monograph Title: Combined Arms in the Electromagnetic Spectrum: Integrating Non-Kinetic Operations

Approved by:

_____, Monograph Director
Robert Tomlinson, Ph.D.

_____, Seminar Leader
Michael J. Lawson, COL

_____, Director, School of Advanced Military Studies
Thomas C. Graves, COL

Accepted this 23rd day of May 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

COMBINED ARMS IN THE ELECTRO-MAGNETIC SPECTRUM: INTEGRATING NON-KINETIC OPERATIONS, by Major Jeffrey C. Crivellaro, USAF, 47 pages.

Anti-access, area denial (A2AD) environments provide adversaries with an asymmetric advantage too costly for a 21st - century military to overcome. Arguably, a counter to a defense-in-depth environment is an attack-in-depth strategy. However, regaining a relative advantage requires leveraging the electro-magnetic spectrum to offset the high cost of traditional targeting methodologies. This monograph suggests a framework for negating an anti-access, area denial advantage by integrating non-kinetic operations to induce strategic paralysis within the enemy's decision cycle. Electronic warfare, computer network operations, and space control negation require the same level of command and control, integration, and synchronization as kinetic fires in order to produce discernible effects on the battlespace.

This paper postulates that there is not a common understanding of what non-kinetic effects encompass. This is because terms like information operations (IO) and non-kinetic effects are ambivalent and do not help military planners bring capabilities to bear as easily as with kinetic operations. In addition, planning and operating in the information environment requires a different perspective from that of traditional, kinetic fires. How do planners create non-kinetic options for the commander that increases relative advantage? One answer is through an examination and synthesis of a proposed evolution of the Clausewitzian definition of *force* with John Boyd's notion of a mental-moral-physical harmony that exists within the cognitive dimension of human decision-making.

This monograph proves that there is a more effective mechanism for targeting outside the brackets of kinetic effects. The employment of electronic warfare and computer network operations throughout the non-kinetic battlespace serve as the mechanism to uncover an adversary's strengths and weaknesses, exploit the friction caused by his inability to cope with unfolding circumstances, and overwhelm the critical connections that provide cohesion. This paper shows that non-kinetic thought links the elements of non-kinetic operations to reduce an adversary's relative anti-access, area denial advantage in the physical domains of air, land, maritime, and space.

TABLE OF CONTENTS

ILLUSTRATIONS

TABLES

INTRODUCTION

Near-peer competitors, such as China, are focusing their efforts to create an anti-access, area denial (A2AD) environment that provides them an asymmetric advantage.[1] The intent of the 21st-century adversary's defense-in-depth is to present multiple barriers that are too costly for the invader to overcome.[2] How can US forces overcome this advantage? This monograph will suggest a framework for negating this advantage by integrating non-kinetic operations to induce strategic paralysis within the enemy's decision cycle. At the operational level, command and control of non-kinetic operations should be centralized, yet decentralized for execution at the tactical level to produce a synchronized effect on the battlespace. This document will also advocate and provide recommendations for developing non-kinetic graduate level academics. The paper will do both by answering the question "what are non-kinetic effects and how do joint military planners integrate them across the realm of military operations?"

This paper suggests that there is not a common understanding of what non-kinetic effects encompass.[3] This is because terms like information operations (IO) and non-kinetic effects are ambivalent and do not help military planners bring capabilities to bear as easily as kinetic operations. For example, when planners identify the need for offensive counter air (OCA) in a campaign, they can define specific parameters to come up with a physical platform that can execute that particular mission. What led to the selection for a kinetic capability in the first place? One answer might lie with partial familiarity of the weapon system; but further analysis shows that ignorance of the existence of available non-kinetic options dominated the decision. A limited understanding of non-kinetic effects will ultimately hinder the planner's creativity and will fail to

---

[1] Jan van Tol, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington D.C.: Center for Strategic and Budgetary Assessments, 2010), 8.

[2] *Joint Publication 3-01, Countering Air Missile Threats* (Joint Chiefs of Staff, 2007), I-8.

[3] *Air Force Doctrine Document 3-12, Cyberspace Operations* (USAF Chief of Staff, 2000), 20.

produce a comprehensive course of action detailing the full gamut of opportunities. Electronic warfare, computer network operations, and space control negation require the same level of command and control, integration, and synchronization as kinetic fires in order to produce discernible effects on the battlespace.

It is important to understand that neither IO nor non-kinetic operations are effects unto themselves. They are terms, doctrinal as in the case of IO and thoughts defined in this paper as in non-kinetics, which refer to specific capabilities. Electronic warfare (EW), computer network attack (CNA), and space control negation (SC-N) are the capabilities, according to this author, produced under the umbrella of non-kinetic operations. However, during detailed operational and tactical level planning, one should not be content with limiting themselves to those finite generalities. For example, it would seem trivial to specify *OCA effects* as a requirement when the planner knows that they'll need attack operations against enemy C^2 nodes with embedded fighter escort, and anti-radiation missiles to counter radar guided surface to air missiles.[4] It would be equally trivial to request *EW effects* when early warning radar denial, air launched decoys, and real-time adversary force disposition was what the planner really required. Thinking of non-kinetic operations in terms of their doctrinal subcomponents provides a clearer understanding of how to produce their unique effects on the battlespace.

The battlespace for non-kinetic operations in defined as the electro-magnetic spectrum (EMS). The EMS is a maneuver space similar to the physical domains of land, sea, air, and space.[5] Energy propagates through the EMS in a wired or wireless medium and spans all of the traditional domains. The intent of non-kinetic operations is to control the EMS at a particular time

[4] Ibid., IV-14.

[5] Robert J. Elder, Lt Gen, USAF (Ret), *21st Century Electronic Warfare* (Association of Old Crows, 2010), 3.

in order to influence, disrupt, corrupt, or usurp an adversary's decision-making capacity.[6] The paper will analyze the types of networks employed to increase the enemy's observe, orient, decide, and act decision cycle. These systems include battlefield, telephony, computer, and industrial control networks. They tie together an adversary's integrated air defense, command, control and communications (C^3) systems, and the critical infrastructure required to sustain operations. The subcomponents of these networks represent critical nodes that must be properly weaponeered, targeted, and apportioned. The integration of kinetic and non-kinetic fires must take place simultaneously through the same planning process in order to synchronize and layer effects during mission execution.

The synchronization of non-kinetic fires requires coordination at both the operational and tactical levels of warfare. This paper advocates for the inclusion of a non-kinetic operations duty officer (NKDO) into the existing air operations center (AOC) construct. This cell will be the focal point for the planning and execution of non-kinetics in conjunction with kinetic fires. It will also provide options for the CFACC as conditions on the battlefield change. The paper will also discuss command relationships at the tactical level that leverage existing air breathing assets. The key concept with the dual operational-tactical approach is to provide the commander with an accurate depiction of the information environment that facilitates timely decision-making.

The final section of the paper encompasses how to weaponeer non-kinetic options from mission analysis through course of action development. There is a need for a holistic, campaign-centric understanding of how Air, Space, and Cyberspace capabilities are weaved/interleaved across the realm of military operations. An anti-access, area denial environment is the backdrop used to showcase the integration of kinetic and non-kinetic operations against a complex problem set.

---

[6] *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms* (Joint Chiefs of Staff, 2011), 163.

Review of the Relevant Literature

Several publications look to inform this study with respect to the complexity of an anti-access, area denial battlespace and the ability of humans to adapt to a dynamic environment. *AirSea Battle: A Point-of-Departure Operational Concept*, published by the Center for Strategic and Budgetary Assessments (CSBA) in 2010 was the stimulus that necessitated the furthering of non-kinetic/kinetic integration. However, anti-access, area denial environments are not anything new, they now span across multiple domains and can produce an asymmetric advantage directly against the way the United States approaches warfare. The AirSea Battle concept explores the interrelationships between domains and exposes the inherent vulnerabilities of being overly reliant on technological advances.

The Scientific Way of Warfare reinforces the ideas of AirSea Battle. Antoine Bousquet, lecturer in international relations at Birkbeck College, University of London, argues that the scientific ideas of current theories and practices of warfare in the Western World were reflections of history.[7] The value of *The Scientific Way of War* is especially important to understanding the US military's association with technology and the significant shortfalls from an over dependence on technological assistance in trying to minimize chaos on the battlefield. In fact, the way of war permeates society to such a degree that it is impossible to separate discourse from reality. For example, Bousquet continues to discuss the parallels between advancement in computer science and the notion that war is controllable. He explains that, in cybernetic warfare, there exists the assumption that overcoming chaos requires an appropriate deployment of negentropic information technology.[8] In risk management, negentropy is the force that seeks to achieve effective organizational behavior and lead to a steady predictable state.

---

[7] Antoine Bousquet, *The Scientific Way of Warfare* (New York, NY: Columbia University Press, 2009), 3.

[8] Ibid., 130. In information theory, Negentropy measures the difference in entropy (disorder) between a current state and an ideal state.

The Soviet Union's development of their integrated air defense system was an attempt to control the human element in warfare. This system completely centralized command, control, communication, and execution in order to mitigate the risks of human error. [9] The basis for this strategy relies on national-level battle management, facilitated by regional digital communications networks, in order to control tactical engagements. Though hardly a Maginot line by any stretch of the imagination, this sophisticated defense-in-depth theory was not without its flaws. As Bousquet points out a pitfall of computer modernization is the notion that war is reducible of to a set of mathematical functions. Thinking that an integrated air defense, precision munitions, or computer-aided systems analysis will reduce uncertainty creates a conceptual framework where chaos is an information deficiency. This theory might work for a closed system where no feedback is required.

Frans P.B. Osinga, Dutch fighter pilot and Senior Research Fellow at the Clingendael Institute of International Relations in The Hague, synthesizes the works of Boyd into an argument for viewing the world as an open system that demands the presence of a competing opponent. Boyd's Observe-Orient-Decide-Act (OODA) loop shows key relationship of how humans evaluate and process information in a dynamic environment. Orientation, central to the theory, is a dynamic process shaping the way humans interact with the environment through a context of cultural tradition, experiences, empathies, beliefs, and goals. Orientation shapes the decision calculus of the present, which then shapes the character of *future* orientation. The present time domain does not confine this dynamic, ongoing and evolving process.[10] Boyd's ideas imply the necessity of a mechanism to aid commanders in comprehending and organizing a multitude of data points to develop an appropriate course of action that accounts for every domain. Therefore,

---

[9] *Air Defense of the USSR*, CIA Historical Review Program, Release as Sanitized (US Central Intelligence Agency, 1999) 5.

[10] Frans Osinga, *Science, Strategy, and War: The Strategic Theory of John Boyd* (New York, NY: Routledge, 2007), 193.

networking organizations in time, space, and purpose provides a common frame of reference.

Linking the theories of Boyd and Bousquet presents a framework for analysis, synthesis, and schemata. This framework ties into the readily available, open-source technical aspects of industrial control systems, telephony, local area network, and modern battlefield communications. The theory argues that the synchronization and integration of electronic warfare, network warfare, and kinetic effects not only shows the relevance of non-kinetic effects, but also of how they influence the commander's planning and decision making calculus. In *21st Century Electronic Warfare,* Lt. Gen. (r) Robert Elder makes a compelling argument for the development and integration of systems and effects that control the EMS. According to General Elder and the Center for Strategic and Budgetary Assessments, the EMS is the next anti-access, area denial environment that will be contested by an opponent that acts like a complex adaptive system. Countering the asymmetric advantage that this contested environment presents requires the synthesis of Boyd's *Organic Design for Command and Control* to visualize a framework that could negate such a complex defense-in-depth strategy.

TYPES OF NETWORKS

The non-kinetic battlespace, as defined by this paper, includes battlefield, telephony, computer, and industrial control systems that operate within the information environment. Figure 1 depicts the relationship between individuals, organization, and systems and how they collect, process, disseminate, and act on information. This cycle ebbs and flows between the physical, informational, and cognitive dimensions through tangible infrastructure, logic data nodes, and analytic processes, respectively.[11] There is a continuous interaction between the information environment, which includes cyberspace, and the physical domains of air, land, maritime, and space. This interaction creates tension between the composite of physical conditions, which

[11] *Joint Publication 3-13, Information Operations* (Joint Chiefs of Staff, 2012), I-1.

influence the employment of capabilities, and the factors that bear on the commander's cognitive decision-making capacity. A commander's ability to manipulate the logical nodes of the non-kinetic battlespace has a direct impact on his capacity to react to changing circumstances.

Figure 1: Conceptualization of activities within the information environment defined by JP 3-13. *Source*: Created by author.

Battlefield networks, industrial control systems, telephony and local area networks—comprised of both physical and logical nodes—enable humans to better evaluate and process information via the OODA loop.[12] The confidentiality, integrity, and availability of information within this construct have a systemic impact on a decision maker's schemata. The goal of non-kinetic operations described in this paper is to delay, disrupt, or corrupt an adversary's OODA loop in such a manner that they cannot bring effects to bear against friendly forces. The desired outcome of incorporating non-kinetic fires into joint planning is to create an asymmetric advantage on the battlefield where it would not normally exist if employment were limited to kinetic-only options. Having a common understanding of each system will provide the context for defining non-kinetic targeting in the section three.

Battlefield Networks

Battlefield networks are a set of integrated C^3 systems that enhance the combat

[12] Dr. Kamal T. Jabbour, *50 Cyber Questions Every Airman Can Answer* (Air Force Research Laboratory, 2008), 6.

effectiveness of fielded forces. This section will use the example of a notional integrated air defense system (IADS) to examine the network's utility within a complex structure. Battlefield networks enable an IADS to detect, classify, analyze, assign, engage, and assess airborne threats that cross into its borders. Figure 2 depicts a cross-section of our notional IADS. It is classified by the three main functions of air surveillance, battle management, and weapons control. Air surveillance is comprised of sensors, such as early warning (EW) radars (figure 2, upper right), that detect, initiate, filter, and combine multiple radar contacts into a single, fused tracking solution that is transmitted over a digital network. [13] For example, an unidentified track is detected by a collection of long-range early warning and height finder radars. Those radars feed an early warning radar company that initiates and merges raw radar data into a coherent radar track that includes speed, altitude, heading, and predicted flight path. It also uses organic systems, such as interrogate friend or foe (IFF), to classify the track as friendly or hostile. A series of similar radar companies (not shown) feed their tracking data into a control and reporting center (CRC). This center filters and fuses tracks to create a common operating air picture for regional commanders within the sector operations center (SOC). The operations center disseminates this common air picture to lower echelons over an air surveillance broadcast (ASB) datalink. The SOC also forwards the air picture up echelon to the area defense operations center (ADOC). Senior leaders within the ADOC can choose to launch airborne interceptors (AI), controlled by ground control intercept (GCI) station, or to let the SOC employ surface to air defenses (or a combination of both.)

[13] *JP 3-01*, V-7 to V-8.

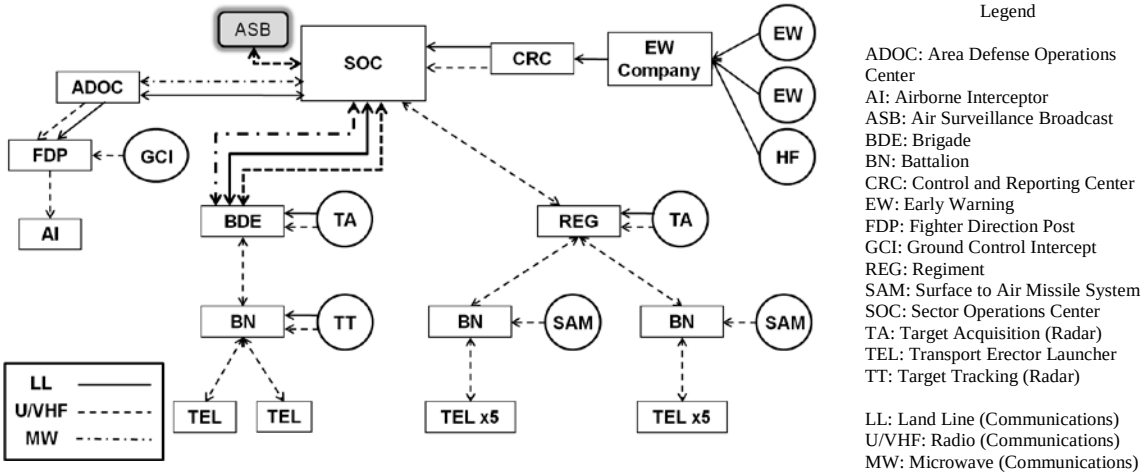


Figure 2: Notional battlefield network within a hypothetical air defense system.

Source: Created by author.

If an engagement with air defense systems is appropriate, the SOC will forward the hostile track and a set of rules of engagement to fielded air defense units such as the fixed, strategic SAM brigade shown in figure 2. Additionally, SOC battle managers have the option to forward target assignments to tactical SAMs protecting deployed ground forces.[14] In either case, both the brigade and regimental echelons have their own organic acquisition radars. Their subordinate battalions are tasked with tracking and engaging the offending aggressor.

Holistically, the design of an IADS maximizes the effectiveness of each unique component within the system in order to protect an area defined by physical boundaries.[15] For example, long-range radars excel at detecting targets, but lack the resolution to guide weapons. The system can automatically hand-off these targets to subordinate acquisition radars when they are within range. This important aspect of an IADS enables the individual radars to radiate for the minimum amount of time to ensure a successful engagement and to increase the survivability of fielded units. In addition, the interconnectedness of air surveillance, battle management, and

[14] Ibid., V-25.

[15] Ibid., I-3.

weapons controls allows a quicker response time to counter ingressing threats. In effect, each component of a battlefield network contributes to shortening the OODA loop of the entire system.

Countering a portion of an IADS does not require destruction of the entire structure. The true area of focus is not the system, per se, but the *ability* of the system to shorten the commander's OODA loop. A physical region could be isolated, thus vulnerable, by neutralizing factor logical nodes within the network. Though section 2 discusses the synchronization of target effects, the key vulnerabilities in an IADS lies in the way it receives, transmits, and processes data between nodes. If the data is disrupted or corrupted, the system will present an inaccurate schema to human decision makers. The consequence is a degraded OODA cycle that renders the system inept for a finite period, over a specified geographical region.

Degrading the OODA cycle requires extensive nodal analysis of key IADS systems. Identifying vulnerabilities allows planners to apply effects to dissect a portion of the network at a given time and place. For example, the radars that feed the EW Company in figure two could be susceptible to noise jamming, false target generation, or IFF spoofing.[16] If the systems at the CRC have access points that touch the internet, then the fused tracking data they forward to the SOC could be vulnerable to corruption. Targeting the microwave data links between the SOC and ADOC with kinetic fires would force the use of landline modems—which possibly traverse commercial networks. The GCI communications used to control fighter aircraft could be jammed to degrade the intercept. Additionally, if the orders and tracks that the SOC is directing to its fielded brigades and regiments is inaccurate, then those units will be less effective at prosecuting their targets in a timely matter. In addition, at these lower echelons, without the situation awareness provided by the SOC, they will need to radiate their organic radars to provide their own targeting solution. This push to autonomous operations decreases survivability and reduces

[16] Adrian W. Graham, *Communications, Radar, and Electronic Warfare* (Wiley, 2011), 99.

overall mission effectiveness.

These examples highlight a few methods of how to degrade a system by attacking the mechanisms that impede decision-making. The IADS scenario is a representation of *traditional* military targeting. The previously mentioned nodes would usually show up on the air component's joint integrated prioritized targeting list (JIPTL) and have forces apportioned on an air tasking order (ATO). Consider the following three systems *non-traditional* in the sense that they are not usually part of an ATO.

Industrial Control Systems

Industrial control systems (ICS) categorize several types of processors, for simplicity, only discussion on supervisory control and data acquisition (SCADA) systems is necessary within the context of joint planning.[17] SCADA systems control geographic dispersed assets where central management is critical to operations. These systems can include oil/gas pipeline, water, electrical power grid, and railway transport distribution. A SCADA system performs centralized monitoring and control of remote sites over long-distance communications networks. The remote sites provide feedback to a central hub that can push supervisory commands to control field devices. These devices can open and close valves/breakers, collect sensor data, and monitor local conditions.

Without diving into the complex details of a SCADA network, the system can be broken down into three main components. There is a primary control center, hundreds of remote stations, and the communications pathway that provides connectivity.[18] Think of the control center as a computer network with workstations and control servers. At the remote station end, there are modems, computers, sensors, and controllers that operate valves, pumps, turbines, etc. For

[17] Keith Stouffe, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems Security* (US Department of Commerce: National Institute of Standards and Technology, June 2011), 2-1.

[18] Ibid., 2-7.

example, an electrical power grid has several remote stations that provide power distribution to a specified region. The control of each station occurs centrally to ensure each is operating within a finite set of parameters. Communications between them usually occurs via satellite, radio relay, cellular, telephone lines, or even over the internet. More and more modern ICS are replacing proprietary equipment with internet protocol solutions.[19] This could potentially subject a ICS, such as a SCADA network that controls power distribution to military facilities, to internet accessible vulnerabilities.

As with an IADS, extensive nodal analysis is required to understand the type of ICS employed, how it functions, and how it is remotely accessed/controlled. For example, after months of network reconnaissance, it might be possible to isolate the specific remote stations that supply electrical power to military facilities such as an airbase, its radars, defenses, communications systems, or operations center. Non-kinetic targeting of these specific stations produces an asymmetric advantage against an adversary while minimizing potential collateral infrastructure damage. The next section will revisit the implications of targeting SCADA and power distribution systems.

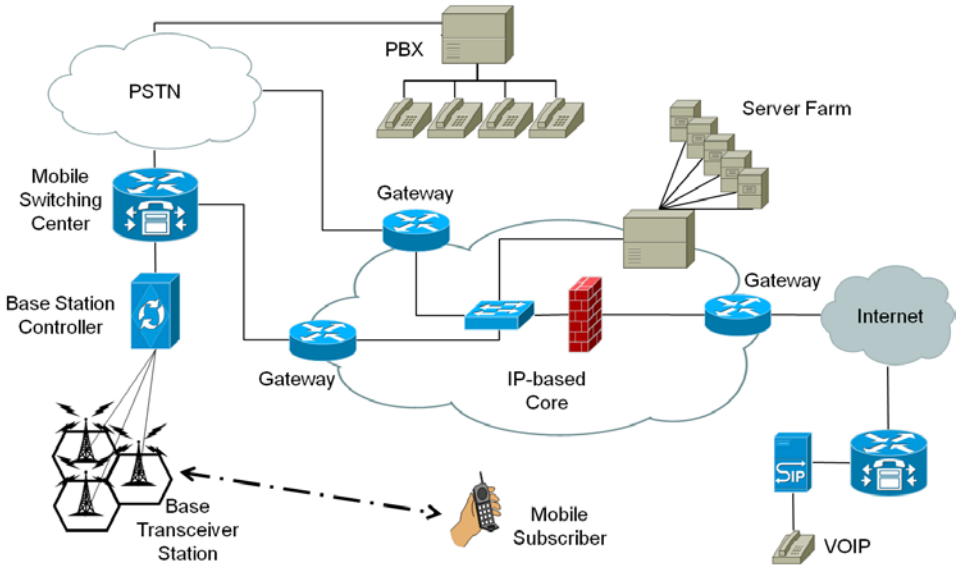
Telephony Communications

The second *non-traditional* military target is telephony communications. Figure 3 represents a modern mobile subscriber network typically seen in urban environments.[20] The diagram shows the relationship between mobile, landline, and internet telephony. The easiest method to breakdown this network is to start with the mobile subscriber and to go through the steps of initiating a call event. As a mobile device powers on, it attempts to register with the cellular network. Nearby cell towers (base transceiver station–BTS) listen for this request and

[19] Ibid., 3-1.

[20] Marc Orange and Brough Turner, *3G Tutorial* (NMS Communications, 2002), 43.

forward the subscriber's identification to the base station controller. The controller determines the subscriber's location via the phone's GPS data or its timing advance from each cell tower as communicated from each BTS.[21] The controller uses this information to assign the subscriber to the optimal tower for communications. Before it finalizes the assignment, the controller verifies the subscriber's identity with the mobile switching center (MSC). The MSC is the heart of the network's operations. There is usually one per city per service provider. The MSC acts as the gateway through which subscribers communicate across the same cell network, onto traditional landline phones, or through the internet.



PBX: Private Branch Exchange (telephone network within an enterprise used to share a certain number of outside lines)
PSTN: Public Switched Telephone Network (circuit-switched network that sets up dedicated channels between two points for the duration of a call)
VOIP: Voice over Internet Protocol (packet-switched telephony over the internet)

Figure 3: Basic 2.5G telecom network.

Source: Created by author.

For example, if a mobile subscriber initiates a call intended for a recipient with a landline phone, the event begins with BTS channel allocation. The BTS transmits the call data–to include

[21] Ibid., 82. Timing advance refers to a phone's distance from a GSM tower. The network needs to know a phone's location in order to assign it to the correct tower and to calculate the optimal power settings for the phone and tower to conduct communications. The base station controller performs this continually as the subscriber travels from tower to tower.

digitized voice, location, identification, and other data messages–to the controller and then to the MSC. The MSC determines if the intended recipient is on the cellular network or if it belongs to another carrier. Since the number dialed belongs to a landline-based carrier, it forwards the call to the public switched telephone network (PSTN). Think of the PSTN as a cloud of interconnected circuit switches that activate in a manner to establish a physical link between two nodes for the duration of the call. The two nodes in this case are the MSC (connected to the mobile subscriber) and the recipient's phone. If the recipient is within a corporate organization–or military base–the PSTN creates a circuit to the organization's private branch exchange (PBX). The PBX then establishes a circuit to the recipient's phone. A PBX allows users to share a limited number of external phone lines and acts as an internal phone network for an organization.

Mobile services providers also allow their subscribers to access the internet. The MSC handles communications in a similar manner as with the previous example. If the user wants to access a webpage, or initiate a voice over internet protocol (VoIP) conversation–such as a service like Skype–the MSC opens a gateway to the internet. The section in *figure three* labeled *IP-based cloud*, represents a collection of logical nodes that provide network services, such as email, downloadable applications, and streaming media, to subscribers. It also is the access point into the internet.

The critical aspects of this telecom network are first, the MSC logs the location of all of subscribers on the network. Second, the MSC, in order to provide advanced services, connects users to the internet through an IP-based core. Third, the MSC connects to the PSTN in order to route subscribers to external landline phones. These three nodes represent potential vulnerabilities. For example, network subscribers could be located and identified through the compromise or subversion of the gateways, routers, and firewalls between the MSC and

internet.[22] Telephone network attacks (TNA) throughout the PSTN could interrupt mobile and landline call events. Finally, a compromised PBX could severely degrade an organization's telephony communications. The usefulness of these aspects to the military planner comes with understanding an adversary's pattern of life. The planner needs to know which nodes to effect in order to manipulate the adversary's telecommunications network.

Local Area Networks

The final set of *non-traditional* military targets is contained within local area networks (LAN). A LAN is made of layers of servers, workstations, switches, routers, firewalls, and the communications medium that connects it all together. For simplicity, the discussion on LANs is with respect to the previous systems described within the non-kinetic battlespace. *Figure 4* depicts a LAN with access points into the internet, PSTN, point-to-point communications, and an ICS network. The previous section on SCADA mentioned how point-to-point communications connect geographically separated networks. Consider a very small aperture terminal (VSAT) as a type of point-to-point satellite communications medium that connects geographically separate LANs into a seamless network.

[22] Jason Halpern, *IP Telephony Security in Depth* (Cisco Systems, 2003), 12.

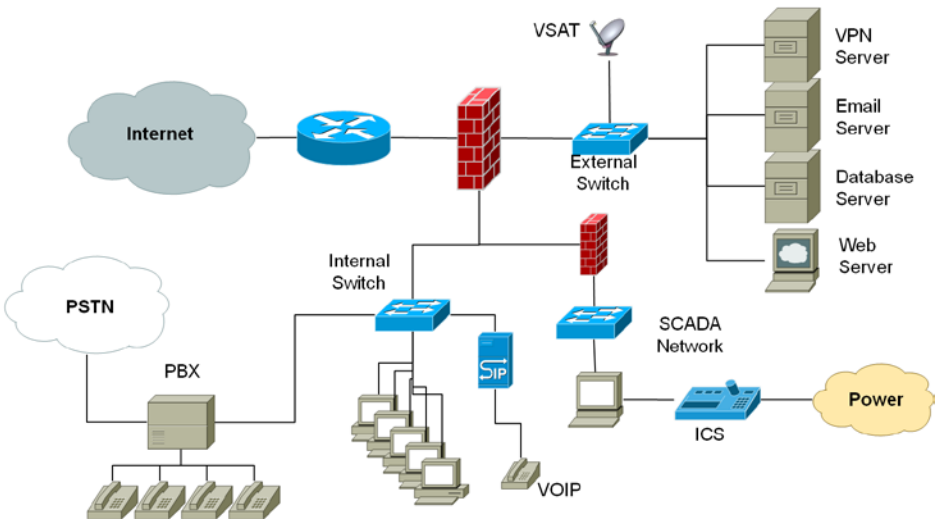


Figure 4: Local Area Network.

Source: Created by author.

As already mentioned, a LAN connects various systems together to provide services, such as communications, remote access, remote monitoring, and central management. Think of the networks inside of an operations center. For example, there are landline phones, VoIP phones, terminals with data feeds from remote facilities, and systems that control RF communications. Additionally, in figure four, replace the icon labeled *power* with HVAC, or replace the entire segment labeled *SCADA network* with *interface to battlefield network*. Think of the potential vulnerabilities to such a complex, interconnected system. A few that come to mind for the military planner are access points from the internet or from the PSTN. Misconfigured or corrupted access controls could allow subversion of the center's internal phone system, display terminal, radio control, email, datalinks, or remote monitoring capabilities. Think of the ramifications of unknowingly commanding subordinate units to target friendly aircraft or orders that a never heard by fielded forces. If this was a sector operations center within an IADS, battle management would be severely impeded, which would result in a slower, less effective OODA loop.

Additional targeting options are revealed to joint planners as IADS linkages and the networks that facilitate its ability to process high volumes of data are uncovered. Not only could radars and radio be jammed to degrade an air defense, but phones, servers, routers, electrical power, and battlefield networks could be corrupted or disrupted to invoke shock within the heart an adversary's decision cycle. To this point in the monograph, the IADS has been the central theme, but it is not the only system susceptible to non-kinetic operations. The key is to focus on integrating non-kinetic operations to paralyze the adversary's OODA loop in a manner where they cannot act in time to be effective. Battlefield networks, industrial control systems, telephony, and LANs present interconnected access points that tie directly into the decision cycle. They are an additional targeting avenue to consider and synchronize alongside kinetic fires.

SYNCHRONIZED EFFECTS

How does one go about delaying or preventing enemy action? It isn't enough to merely integrate effects—non-kinetic operations must be layered and synchronized in time and space. These operations must focus on critical access points that, when acted upon, cause a systemic reaction that adversely effects the enemy's decision cycle. The easiest way to show this level of synchronization is to step through an example of a notional tactical engagement. This section walks through the layering of effects to highlight the benefits of simultaneity. There are two main concepts to pull from this section. First, network reconnaissance requires months of prior exploitation to manifest these effects on the battlespace. Second, centralized operational coordination and control is required to execute these complex tasks at the tactical level. The following example uses the targeting examples from section 2 to illustrate the layering of effects, by phase, in a notional engagement.

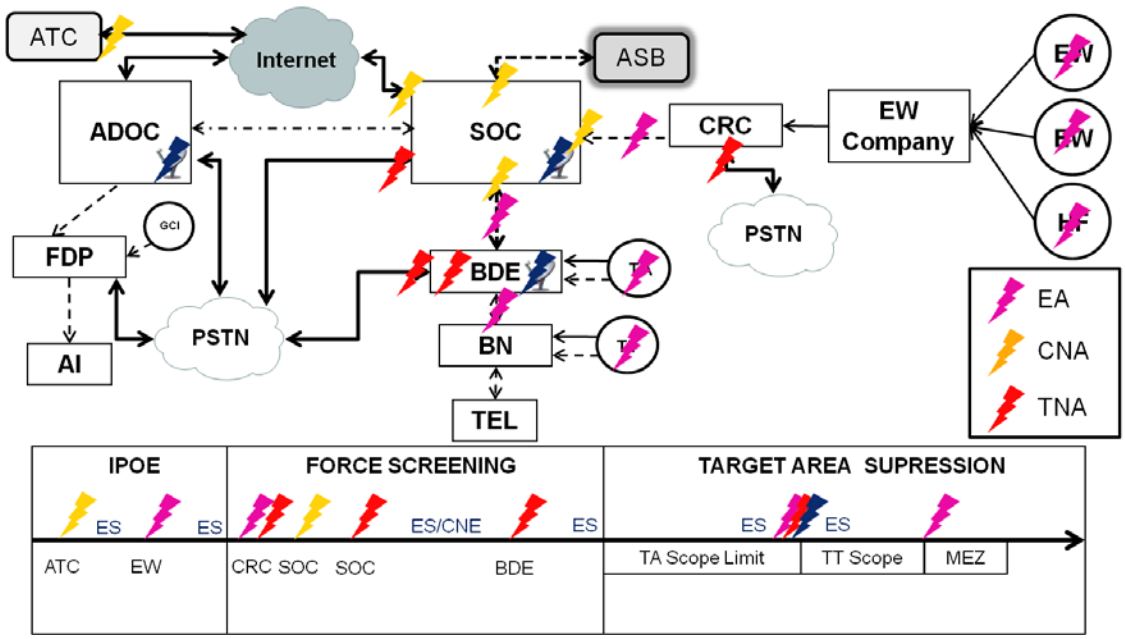


Figure 5: Synchronizing effects by phase.

Source: Created by author.

The objective in our notional mission is to enable ingressing aircraft to destroy high valued targets, under a SAM brigade's (BDE) umbrella of protection, within a sector of an IADS depicted by figure 5. The three mission phases in this example include intelligence preparation of the operational environment (IPOE), force screening, and target area suppression. The goal of the IPOE phase is to determine the enemy's disposition.[23] Some of the predictors of an opponent's current state could include indicators such as weapons control readiness levels, geographical deployment conditions, and changes to the amount of military communications within the battlespace. It also includes the discovery of new operating radio frequencies, IP addresses, phone numbers, and digital datalinks that differ from pre-briefed intelligence reports. A plausible assumption during the IPOE phase is that operational and nation-level command and control authorities most likely will not employ their organic early warning radars nor will the subordinate brigades radiate their acquisition radars. Deriving this assumption requires knowledge of enemy

[23] *JP 3-01*, III-1.

operating procedures and doctrine that reveals how the system balances speed versus survivability.

Knowing the adversary's doctrine and tactics provides a level of expectation for the non-kinetic planer. For example, without organic radars, the enemy's operations center should be receiving situation awareness through civilian air traffic control (ATC) radars and other passive means. This assumption fits the notion of how an IADS would maintain survivability.[24] Knowing that maintaining accurate situation awareness is crucial to an IADS success, a probing attack, such as using a computer network exploit to deny its IP-based ATC connection, should provoke a reaction.[25] Without connectivity to the remote air picture, which jeopardizes rapid command and control, subordinate centers and radar companies might be ordered to radiate long-range systems to derive their own organic operating picture. Reconnaissance assets would be on station to notice this change within the enemy's system. Also, the collection of these new communications and radar frequencies could be used by airborne jamming platforms in follow-on mission phases.

The network attack just described is but one method of a layered approach in stimulating the area defense system. The telecommunications architecture presents another vector for inducing confusion between the echelons of this complex network. For example, degrading the modem and voice communications between strategic and operational level command authorities disrupts the command and control of subordinate brigades and fighter direction posts. This could result in those entities moving to a more vulnerable means of communications.[26] These, newly discovered open-air voice and datalink frequencies, when further exploited, present a possible targeting solution for use during the force screening phase.

---

[24] Dr. Carlo Kopp, *SAM System Mobility: Russian and PLA Air Defense System Vehicles*, Technical Report APA-TR-2008-0601 (Air Power Australia, 2012), 2.

[25] Dr. Kamal T. Jabbour, *50 Cyber Questions*, 9.

[26] Jason Halpern, *IP Telephony Security in Depth,* 4.

As strike aircraft arrive on station, jamming platforms could degrade early warning voice and radar systems to mask the presence of friendly assets. Simultaneously, the servers and routers that control communications equipment and battlefield network terminals should experience a denial of service due to a synchronized computer network attack. The additional layers of non-kinetic fires further compounds the adversary's OODA loop and isolates key battle management decisions from reaching subordinate units.[27] In the absence of these non-kinetic effects, the expected enemy reaction would be a rapid response from the leadership echelon to subordinate units—translated into alerting surface to air missiles sites and scrambling enemy fighter aircraft. Delaying these actions by inducing strategic paralysis in the decision cycle buys time for friendly attacking aircraft to access enemy airspace without a significant hostile reaction.

As the air defense brigade becomes isolated from its command and control, based on previous discussion, a reasonable expectation is that they will radiate their organic target acquisition radars to find, fix, track, and engage their own targets. Attacking this network requires some basic background into its concept of operations. Figure 6 shows a notional target engagement timeline. In this example, the acquisition radar has a detection range of 100 miles. The air defense brigade assigns and hands-off the target to the appropriate firing battalion once it is about 50 miles away. This distance corresponds to the maximum detection range of the air defense battalion's target tracking radar. The assigned unit, using the acquisition data from its headquarters, waits to radiate its tracking radar until the target is within the missile engagement zone (MEZ). This minimizes radiation time and enables the system to track, engage, and assess its target as efficiently as possible.

[27] Dr. Kamal T. Jabbour, *50 Cyber Questions*, 13.

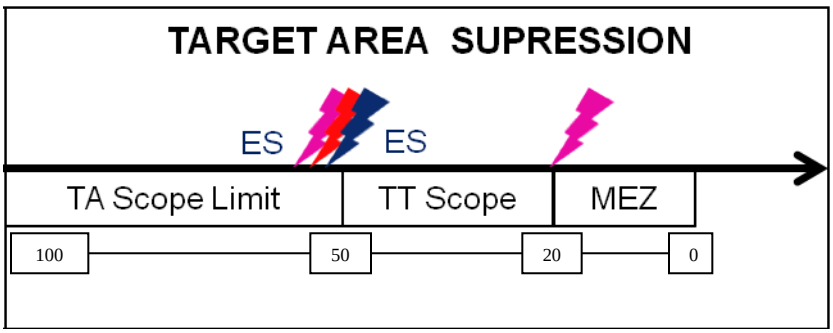


Figure 6: Notional Target Engagement.

Source: Created by author.

The lightning bolts on the figure 6 represent critical times to inject confusion into this tightly controlled process. Preventing a positive hand-off from brigade to battalion will deny cueing of the target tracking radar. If the battalion loses voice and datalink communications with the brigade, they will be forced to operate autonomously. Under these conditions, the expectation for the battalion is to radiate its tracking radar to acquire its own target organically. Consequently, this specialized radar is ill suited for target acquisition.[28] It will have to radiate for a longer duration decreasing survivability to conventional and anti-radiation munitions.[29] Another consequence of early and continuous radiation is that the battalion is broadcasting its position for intercept by collection assets. This aids the cueing of electronic attack assets and allows them to better posture themselves for jamming the system when the friendly aircraft is inside the missile engagement zone. As a result, the denied engagement allows friendly aircraft to bypass the threat and strike their targets.

In this sample intercept, delaying command and control, cueing, and weapons control degraded the IADS at key times in order to prevent a successful hostile engagement. Think of this example as a sort of template for the employment of non-kinetic operations on a notional

[28] James C. O'Halloran, *Jane's Land-Based Air Defense* (Janes Information Group, 2011), 127.

[29] Dr. Carlo Kopp, *SAM System Mobility: Russian and PLA Air Defense System Vehicles*, 4.

battlespace. Chance and hope should not dominate the realization of these effects. The synchronization and simultaneity of non-kinetic effects are crucial in conducting any type of operation. Even in its simplicity, many moving parts must be carefully coordinated and controlled in order for execution to be successful.

NON-KINETIC OPERATIONS INTEGRATION

In order to achieve the cumulative effects of non-kinetic operations, the JFC needs a mechanism to synchronize and integrate capabilities at the component-level. The conduct of non-kinetic operations should be no different from traditional kinetic engagements. In fact, this paper argues that non-kinetic operations remain within the bounds of the joint force component construct.[30] As compared with joint information operations, the components should normally be responsible for the planning and execution of non-kinetic operations.[31] The joint force component commander will establish the parameters for functional commanders to plan and conduct these types of operations.

Assuming that the air component has the preponderance of non-kinetic operations assets, the CFACC will be delegated the authority to plan and execute these operations from the combined air operations center (CAOC). This does not mean that non-kinetic planning should be absent at the JFC level. In fact, the joint operations center's J3 should have NK planners on staff to build NKO into the campaign plan from the beginning. This section advocates for a new duty officer section within the combat operations division (COD) in order to centrally command and control non-kinetic operations in support of JFC objectives.

Non-Kinetics Duty Officer Team

The non-kinetics duty officer (NKDO) team would be the focal point for non-kinetic

[30] *AFDD 3-12*, 21.

[31] *JP 3-13*, xii.

operations in the COD. The NKDO is responsible for executing applicable portions of the ATO and making C2 decisions to ensure commander's objectives and intent are satisfied. The NKDO closely coordinates with other members of the COD and directly manages the employment of CNA, SC-N, and EW capabilities. The NKDO team, as depicted in figure six, would consist of the NKDO, Space Control Coordination Element (SCCE), Cyber Control Coordination Element (CCCE), Electronic Warfare (EW), Non-Kinetic platform LNOs (when required), and an airborne commander acting as an extension of the NKDO.[32] The NKDO would execute from the combat operations floor, with a portion of the team in a classified facility. Individual elements, such as space and cyber units execute their tasks while geographically separated.

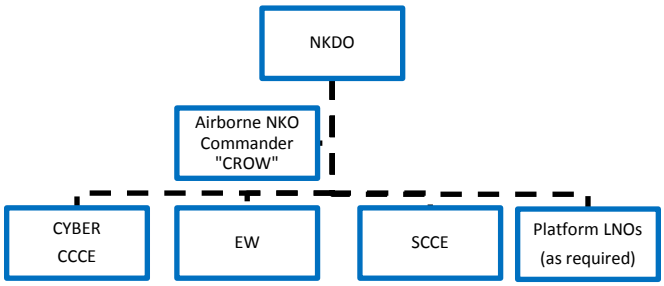


Figure 7: Non-kinetic duty officer team organization.[33]

The NKDO would work directly for the chief of combat operations (CCO) and would be the single voice for non-kinetic issues in the COD. Duties include monitoring the current offensive/defensive non-kinetic situation and its interaction with the air, land, and sea domains. The NKDO would also advise the CCO of dynamic mission requirements, resources and status and recommending immediate changes to the ATO that are in accordance with JFC or CFACC guidance. The NKDO would provide non-kinetic inputs to the air components lines of operation and would support planning at the JFC level as directed. Additionally, the NKDO would coordinate, through tactical C2, mission critical information to relevant package commanders, as

[32] *AFTTP 3-3.AOC, NKDO Team Section* (US Air Warfare Center, Draft 2011), 4.

[33] Ibid.

required.

The NKDO is responsible for synchronization and coordination of non-kinetic operations throughout the ATO execution period. This may include but not be limited to: re-tasking of non-kinetic assets to support dynamic targeting (DT) or personnel recovery (PR) operations, evaluating the impacts of non-kinetic targeting changes, satisfying reactive requests from components and monitoring current operations to ensure non-kinetic assets made available to the CFACC are being effectively employed. The NKDO must also have a strong understanding of the ATO process, AOC procedures, Cyber Tasking Order (CTO), Space Tasking Order (STO), air operations, and the integration of all non-kinetic capabilities into the realm of military operations.

The airborne NKO commander, callsign CROW, serves as an extension of the NKDO. Though this position may not be required for all operations, it can enhance operational level situation awareness by having data pushed directly from an airborne conduit. Both planning and execution require the integration of the CROW. This position can act as a backup mechanism for C^2 of NKO if connectivity with the AOC is degraded. The primary duty of the CROW is to coordinate atmospheric EMS effects with airborne electronic warfare assets.

The space and cyber control coordination elements will receive requested effects and calls for fires from the NKDO. They will be responsible for the execution of pre-planned/pre-approved space and cyberspace control effects, respectively. In the event of a non-pre-approved dynamic or emerging target, the NKDO will direct coordination with JFCC-Space and/or USCYBERCOM as appropriate, for required execution authorization.

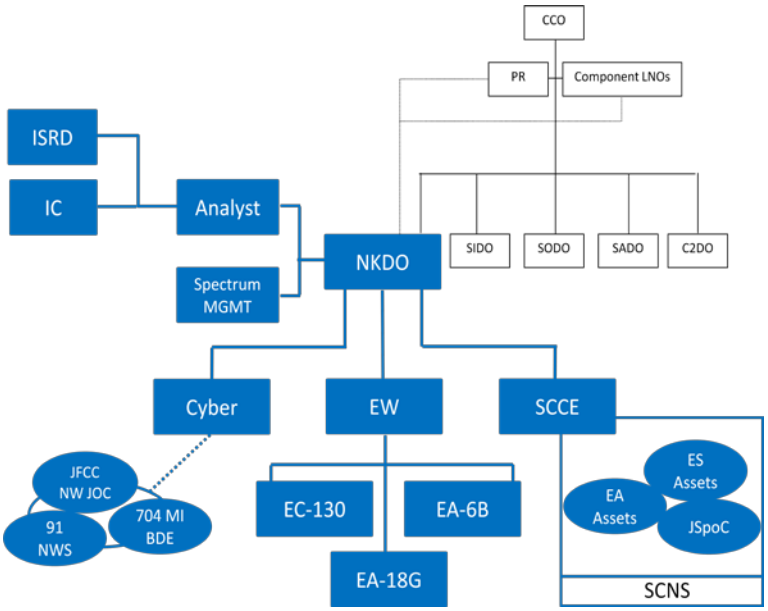


Figure 8: Non-kinetic duty officer hierarchy.[34]

NKO Integrated Planning and Execution

In addition to executing from the COD floor, the NKDO team will allocate planners to integrate NKO effects into the remainder of the Joint Air Tasking Cycle (JATC). For example, the NKDO will be responsible for providing feedback to the NK planners on any indications that can help assess the defined measures of performance and measures of effectiveness for given tactical task. These indicators are critical for assisting the strategy division in formulating an air, cyber, and space apportionment recommendation that fully considers the current effectiveness of available non-kinetic options.[35]

To maintain a holistic targeting strategy, the NKO target development planner will work with the ISR division targets and tactical assessment team to provide target nominations to

[34] Ibid., 8.

[35] *JP 3-30*, III-23.

achieve CFACC objectives through kinetic or non-kinetic means.[36] During target development, the NKO target development planners will analyze the non-kinetic options for effecting adversary systems. After analysis is complete, the identified target set is prioritized and submitted as part of the prioritized Target Nomination List (TNL). A thorough understanding of the adversary's nodes, C2, and centers of gravity will aid in selecting appropriate non-kinetic effects to achieve objectives. The NKO target developer will pass a non-kinetic integrated joint integrated prioritized target list (JIPTL) to the master air attack plan (MAAP) NKO planner for the allocation process in the MAAP. This hand-over quickly focuses the MAAP NKO planner to detailed non-kinetic related targets during the MAAP planning cycle.

Integrating NKO into each stage of the JATC is required to facilitate synchronization in a complex scenario, such as the one described in section 3. The NK planning team–through apportionment, targeting, and allocation–consolidates the integrated non-kinetic battle rhythm into the overall air strategy. The NKDO's most challenging part of execution is the decision portion of his OODA loop. The NKDO needs tools, similar to the CFACC and JFC, to facilitate timely and accurate decision-making. As with any plan, the commander needs embedded options to mitigate risk. At the low operational, high tactical levels of war, these options are similar to the branches and sequels of the campaign plan. The decision support matrix (DSM) is like a playbook that provides the NKDO and the CFACC a set of criteria to better gauge when to issue orders.[37] The sample DSM presented in Table 1 provides an example of how the NKDO should focus ES collection, through coordination with the ISR division, to fulfill a commander's critical intelligence requirement (CCIR).[38] It also creates a shared mental model between the NKDO and the CFACC on the triggers for requesting and executing higher-level. This minimizes risk by

[36] *AFTTP 3-3.AOC, NKDO Team Section* (US Air Warfare Center, Draft 2011), 22.

[37] Dr. Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity for Decisive Action* (Air University Press 2012), 91.

[38] *JP 1-02*, 62.

helping them visualize the non-kinetic scheme of maneuver.

Table 1: NKO Decision Support Matrix

DP	Phase	NAI	Event	Decision Required	Decision Criteria	Assets	NKDO/CFACC Actions
3	Phase 3 (Target Area)	SOC	2nd SAM BDE cueing off of sector ATC, EW radars, or passive systems– through the SOC–via digital datalink	Authorize NKDO to execute *CNA option B* to deny battle management of and cueing to 2nd SAM BDE	1. 2nd SAM BDE receives target assignment 2. Delayed 2nd SAM BDE acquisition radar 3. 23rd SAM BN passive tracking detected	ES CNA National	1. CFACC authorizes use of *CNA option B* 2. NKDO executes *CNA option B* 3. NKDO alerts CROW to refocus ES collection
Notes:	Assumes GCC/SECDEF has pre-approved CFACC to execute *CNA option B* Assumes cyber forces are postured to execute *CNA option B* on order Assumes "Event" is a pre-planned CFACC CCIR						

Source: Created by author.

The decision required in Table 1 is for the CFACC to authorize the NKDO to execute a CNA option that would deny the battle management of a critical BDE SAM system. The criteria was derived from knowing the enemy air defense force's disposition and knowing the current capabilities of friendly ES and national systems during the target phase of the mission. For example, the NKDO needs to maintain awareness on the effectiveness of his original plan to isolate the SAM BDE. He also needs to know if his assets are capable of determining if the enemy adapted to his plan, in an unexpected manner, especially during the most critical phase of the mission. Effective decision-making requires an understanding of both enemy and friendly forces.

The NKDO needs to be a team coequal to the senior offensive duty officer (SODO), senior air defense officer (SADO), and senior intelligence duty officer (SIDO) in order to confront the complexity of directing and synchronizing non-kinetic operations. At this time, the SODO does not have the expertise available to C^2 non-kinetic operations in a holistic manner. The AOC's current construct spreads cyber-like expertise across each individual division. The SODO may not be able to fully leverage the Information Operations (IO) cell because it does not always include computer network attack specialties. The same is true of space control. The

NKDO team is the combination of these disparate positions. It would also pull the existing electronic warfare coordination cell (EWCC) into the group. Consolidating electronic attack, electronic warfare support, CNA, and space control under one entity for planning and execution provides the CFACC with tangible options that translate into combat power on the battlespace.

The NKDO is one perspective on solving the administrative deficiency of how to command and control non-kinetic operations. It addresses the complexity of the systems discussed in section 2 and walks through the process of executing the synchronization expounded upon in section 3. Yet, how does the NKDO team create tangible options for the CFACC or JFC? Answering this question requires a deeper understanding of the differences between traditional, kinetic thinking and the notion of non-kinetic thought. Though both kinetic and non-kinetic operations can produce a cumulative indirect effect, such as gaining air superiority, they traditionally directly target an adversary's physical capacity—destroying individual enemy air defenses.[39] Non-kinetic thought, on the other hand, examines the consequences of influencing an adversary's cognitive capacity to use those weapon systems effectively. The idea of non-kinetic thought requires a different perspective from that of traditional fires.

FRAMEWORK FOR DEVELOPING "NON-KINETIC THOUGHT"

Clausewitz said, "War is an act of force to compel an enemy to do our will." Force, then, is the mechanism that can shape and change an adversary's way to thinking. Yet, this monograph diverges from Clausewitz's fundamental notion of the term *force* and defines it as any kinetic or non-kinetic effect on the battlefield, employed in a deliberate manner to delay, disrupt, corrupt, or destroy an adversary's decision-making process.[40] As stated earlier, these effects manifest primarily through both the physical domains of land, sea, air, and space, as well as through the

[39] *AFDD 3-1*, 7.

[40] John Boyd, *The Essence of Winning and Losing* (unpublished presentation, draft version 1995), 4. This theory uses Boyd's OODA Loop to define the decision cycle.

electro-magnetic spectrum. The operational artist must understand how to link non-kinetic capabilities across all of these domains through the manipulation of the cognitive dimension.[41]

If operational art lies at the intersection of tactical and strategic thought,[42] then the cognitive dimension is what joins the nodes of the logical realm to the realities of the physical world. The value of non-kinetic operations relies on understanding how to operate within the cognitive dimension. When considering the utility of non-kinetic effects, the operational artist must be mindful of the disproportionate cognitive tension that exists between the physical, logical, and cognitive dimensions of warfare. Clausewitz would say that fog and friction are the products of the conflict between the abstract and the actual characters of war.[43] The operational artist's goal is to account for the variables that could affect fog and friction by integrating non-kinetic effects to increase the confusion in the enemy's decision cycle. In this regard, the application of force is through the asymmetrical apportionment of non-kinetic combat power to gain a localized advantage that collapses the adversary's means to resist.

Time, space, and purpose bound the collapse of the adversary's means to resist and a relative increase in advantage. Having a non-kinetic mindset allows the operational artist to link elements of the logical dimension with those of the physical world. Operational art uses genius—the distinctive cognitive faculties of collective skill, knowledge, experience, creativity, and judgment—to ease the cognitive tension inherent of complex adaptive systems. These systems, Shimon Naveh argued, were the impetus to a paradigm shift from a deductive mind-set, to a systematic, holistic approach to military thinking.[44] Similar to the connection between strategic

---

[41] *JP 3-13*, viii.

[42] Everett C. Dolman, *Pure Strategy* (New York: Frank Cass, 2005), 30.

[43] Carl von Clausewitz, *On War*. Ed. and trans. Howard, Michael and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 101.

[44] Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory*

and tactical thought, non-kinetic thought requires a synthesis, instead of a summation, of the conceptual, logic-based systems—battlefield networks, industrial control systems, telephony, and local area networks—with the traditional, physical-based systems such as fielded forces, logistics, and factories. This mind-set opens new avenues of exploration in an effort to order the tension pervading the cognitive dimension.

John Boyd's describes influencing tension through the idea of breaking down cohesion. Increasing the fog and friction within an adversary's decision cycle requires a penetration of their moral-mental-physical being. The use of force in a direct attack against an opponent's will might prove counterproductive. Planners must focus on the cohesion that exists between the interactive bonds that allow an adversary to exist as an organic whole.[45] Inducing confusion and collapsing his will to resist necessitates the severing of theses linkages by denying, degrading, deceiving, disrupting, or usurping the moral-mental-physical connections that he depends upon.

Boyd explains the idea of destroying an adversary's moral-mental-physical harmony through the synthesis of lethal effort, maneuver, and morale.[46] The objective within each component is to drain an adversary's strength, exploit critical vulnerabilities, and to create the conditions that saturate human action with indecision. The employment of electronic warfare and computer network operations throughout the non-kinetic battlespace serve as the mechanism to uncover an adversary's strengths and weaknesses, exploit the friction caused by his inability to cope with unfolding circumstances, and overwhelm the critical connections that provide cohesion.[47] Commanders and planners need conceptual tools to array non-kinetic action in time, space, and purpose to achieve these desired effects.

(Portland, OR: Frank Cass, 1997), 3.

[45] John Boyd, *Patterns of Conflict* (unpublished presentation, draft version, 1982), 137.

[46] Frans Osinga, *Science, Strategy, and War: The Strategic Theory of John Boyd,* 178.

[47] Ibid., 176.

The Non-Kinetic Toolkit

The only difference between kinetic and non-kinetic planning is the mind-set of the operational artist. Arguably, it is unwise to think about planning as a dichotomy of kinetic and non-kinetic actions. Instead, the two realms require the same consideration when applying the elements of operational design to facilitate the development of courses of action for the joint commander. For example, during center of gravity analysis the same considerations for neutralizing key nodes should be weighted equally between all available options.

Table 2: Operational center of gravity—notional air surveillance

COG	**Critical Capabilities**	**Critical Requirements**	**Critical Vulnerabilities**	**Δ=Decisive Point**
IADS	Air Surveillance	EW Radars	• Dispersed along regional borders • Poor EP	1. Factor radars neutralized
		Connectivity	• Microwave Relay between sites • Commercial fiber optic lines between BNs and filter center • Shared with civilian TELCOM	2. Key sensor linkages disrupted 3. Filter center connectivity subverted
		Power Generation	• Shared with civilian infrastructure	4. Power generation selectively degraded

Source: Created by author.

How does the planner know that a specific vulnerability exists and that it is susceptible to non-kinetic action? Critical factor analysis, as depicted in the notional IADS on Table 2, connects systems analysis of a military center of gravity to the objectives and effects derived from the commander's intent. In this scenario, the notional IADS's air surveillance critical capability allows it to determine the disposition of coalition aircraft. This undesired effect—from a friendly perspective—negatively affects any objective focused on air superiority. The adversary's air surveillance capability requires early warning radars, connectivity between echelons, and power generation at the radar sites and control centers. Attacking these nodes degrades the IADS ability to perform long-range engagements. However, which node is vulnerable and which one is not?

Determining vulnerability relies on asking the right kinds of questions. If a planner were

thinking about using a destroy defeat mechanism,[48] then the questions would have a kinetic flavor: Is the target hardened? Is it in a known location? Is it mobile? Are there redundant communications? How long can it function on backup power generation? All of these questions are relevant and the answers would help facilitate kinetic options. In fact, all of the components may be vulnerable to physical destruction, but the commander may have to factor both strategic and theater restraints. Strategic guidance might dictate minimizing collateral damage and the commander's intent might impose restrictions on striking dual-use targets. Additionally, finite resource such as sorties, standoff munitions, and other competing priorities dictate available kinetic options. However, this mind-set is not enough to qualify as non-kinetic thought. How does one think non-kinetically? How does one formulate a non-kinetic question?

Boyd's moral-mental-physical model pushes the planner to focus on the variables that would most affect the adversary's decision calculus.[49] The real target is not the end-point; it is in the mind of the adversary. In this case, it is in the mind of the battle manager trying to make sense of his sensors. This decision-maker operates within a set of expected conditions. He works best when a finite amount of information is available for analysis while expecting the data (radar tracks) to behave within a predefined set of parameters. Confusion and paralysis become more likely when the connection to the sensor is denied, degraded, or deceived in a simultaneous, relentless attack.

---

[48] *JP 5-0*, III-30.

[49] Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 173.

Table 3: Operational center of gravity—notional battle management

COG	Critical Capabilities	Critical Requirements	Critical Vulnerabilities	Δ=Decisive Point
IADS	Battle Management	Centralized Control	• SOCs at known locations • BDE HQs not hardened	1. SOCs isolated/destroyed 2. BDE HQs located/neutralized
		Connectivity	• Microwave Relay between HQs • Commercial fiber optic lines between SOCs and ADOC • Shared with civilian TELCOM • Shared with civilian Internet • UHF tertiary communications vulnerable to EA	3. Key C^2 linkages disrupted 4. Key fiber nodes disrupted 5. Internal BM C^2 subverted
		Power Generation	• Shared with civilian infrastructure	6. Power generation selectively degraded

Source: Created by author.

Now, the question becomes, which cumulative factors would increase confusion and paralysis in the system presented in Tables 2 and 3? If the target is the mind of the adversary, then the objective would be to affect how information is collected, disseminated, and analyzed. Using this understanding, the vulnerabilities would likely exist while data is at rest, data is in motion, or within the infrastructural networks.[50] These categories translate into the physical sensors— as in radar or antenna, the method and medium of transmission, and the networked process that refines the raw data into a usable product for the decision-maker. A non-kinetic thinker would ask questions such as: What types of early warning radars are employed? Do the radar operators employ electronic protection measure to counter jamming? Does the adversary train in an EMS contested environment? How do the radars communicate with the filter centers and sector operations center? Is tracking automated, computer assisted, or manual? How many tracks can an operator maintain at any once? What types of computer networks exist at the headquarters, sector operations center, and filter centers? Are they connected to the commercial internet or PSTN? How are these facilities powered?

[50] Jason Andress, *The Basics of Information Security*, (Waltham MA: Syngress Press, 2011), 74.

Each of the above mentioned questions relate to a notion of data at rest, data in motion, or infrastructure. Each ties to how a human processes information from multiple sources and reacts to changes in their environment. The critical vulnerabilities and decisive points in Tables 2 and 3 focus on denying the linkages to create the conditions that saturate human action with indecision. Indecision, on the part of the adversary, is a desired effect. In an anti-access, area denial environment, the goal is to render the defensive enablers ineffective.[51] If the enemy is unable to find, fix, track, target, and engage friendly aircraft, surface ships, or ground forces, than what is the utility of an integrated area defense?

Non-kinetic thought links the elements of non-kinetic operations to reduce an adversary's relative anti-access, area denial advantage in the physical domains of air, land, maritime, and space. The mind-set of non-kinetic thought focuses on dissolving the enemy's mental-moral-physical being by breaking down the cohesive bonds that make up his decision cycle. This way of thinking should have the same weight of effort as traditional, kinetically focused rational.

Joint planners need to be mindful of non-kinetic operations and how to integration them into campaigns.[52] The synchronization of kinetic and non-kinetic actions generates options for the JFC that produce an increased advantage, denies advantage to the enemy, or, preferably, both. Planners need an understanding of how to control the EMS—in time, space, and purpose—through an exposure to graduate-level academics that build non-kinetic proficiency.

DEVELOPING GRADUATE-LEVEL ACADEMICS

Generating combat power through EMS control requires graduate-level academics that focus on building non-kinetic expertise. This section will pull on the author's experience as a USAF Weapons School instructor to present a road map for constructing a syllabus that is both

[51] Jan van Tol, *AirSea Battle: A Point-of-Departure Operational Concept*, xiii.
[52] *AFDD 3-12*, 23.

exportable and scalable to the joint community. The desired learning objective is to create a joint planner this is well versed in the network topologies discussed in section 2 and is proficient at integrating non-kinetic operations into the joint planning process. Reference the slide deck in the appendix to illustrate how to develop curriculum that is conducive to a building block methodology.

First, the student will need to understand the definition of non-kinetic operations and how they are linked to the fundamental doctrinal definition of information operations. It is important to emphasis the importance of effecting an adversary's decision cycle in order to satisfy JFC objectives. Essentially, non-kinetic operations are no different from the outcome of kinetic effects in that they both impede an adversary's ability to generate combat power against friendly forces. The primary difference is in the medium where non-kinetic operations achieve these effects. In this case, the EMS serves as the maneuver space that links data and information across all the domains.[53] Slides 2 and 3 of appendix A provide the background for linking non-kinetic operations to the EMS to information operations. Slide 4 links each concept into a continual process within the information environment. In this respect, the EMS is a mesh of logical nodes and linkages that the information environment leverages to span its interconnected processes across physical space to produce battlefield effects.

Second, the student must possess a background in the various network topologies that contribute to an adversary's decision cycle. Battlefield, computer system, industrial control system, and telephony networks illustrate four structures that propagate through the wired and wireless EMS. Slides 5 through 15 in the appendix walk a student through the complexity of these communications systems. It important at this point to stress how they can be leveraged by a military entity on the battlefield. The instructor has the option, based on the forum and audience,

[53] Robert J. Elder, Lt Gen, USAF (Ret), *21st Century Electronic Warfare*, 3.

to scale the classification of the briefing to introduce specific capabilities and tactics that are beyond the scope of this research paper. For example, slide 17 shows the networks, previously discussed, and their possible relationship within a notional sector operations center. The slide only highlights what is possible within the realm of physics. It is up to the instructor on how to frame the overall dialogue.

Finally, introduce the student to the command and control of non-kinetic operations theories proposed in earlier in this monograph. Slides 19 through 22 in the appendix discuss the duties and roles of the NKDO. Specifically, slide 21 illustrates how to the NKDO communicates with his team through various methods at differing classification levels. The center of the diagram shows how the NKDO airborne, callsign Crow, communicates with airborne EW assets to facilitate dynamic adjustments to the non-kinetic scheme of maneuver.

The slide deck in the appendix is just one vehicle to assist with instructing non-kinetic operations. The course needs a set of objectives, tasks, and methods to shape the lesson. In fact, this instruction should not be limited to a singular lesson. Since the capabilities of NKO are similar in function to kinetic fires, C^2, and intelligence, teach them in separate lectures.

Table 4: Sample objectives for NKO academics

Task	Objective
1	Understand the employment tactics associated with the units in the DoD that perform EW, CNA, TNA, and SC-N in support of combatant commanders
2	Describe a notional command, control, and communications network architecture to include air defense hierarchy, organization, critical nodes and linkages
3	Describe a notional telecommunications network and how information flows between endpoints
4	Understand, in a generic sense, how industrial control systems process information between devices and monitoring stations
5	Describe the systems that comprise a generic local area network and how information is routed between nodes
6	Incorporate the vulnerabilities associated with the components relative to objectives 2-5 into critical factor analysis during the operational design phase of joint planning

Source: Created by author.

Professional military education (PME) programs, such as the Air Command and Staff College, could incorporate non-kinetic effects planning into their Joint Planning course. Currently

the syllabi offer limited exposure to non-kinetic operations. For example, one academic session is devoted to Richard A. Clarke's, former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, book *Cyber War*. Expansion of this course and others should include instruction on specific case studies of how open-source cyber-attack vectors compromise the confidentiality, integrity, or availability of information systems. Such examples exist in the book *Chained Exploits*;[54] which functions as a sourcebook on performing and preventing attacks through multiple access avenues. In addition, to teach graduate-level operational cyberspace effects, the faculty must be proficient in information systems security. A course, such as the SysAdmin, Audit, Network, and Security (SANS)[55] Security Essentials is taught as part of undergraduate network warfare training by the 39th Information Operations Squadron at Hurlburt Field, FL. This course offers a one-week fundamental background, taught by industry experts, on network topology, defense-in-depth, security technologies, and cryptography. Faculty from any existing PME program would benefit from this course and could export their knowledge into advanced curriculum.

Context is the key element for creating EMS control academics. Understanding how the EMS relates to the traditional domains and how is the medium for influencing the adversary's decision cycle provides a contextual framework for non-kinetic operations. Understanding network topologies provides a visual battlespace that shows context for the logical nodes connected by the EMS. Finally, understanding the planning and execution of non-kinetic operations provides relevance to the joint planner on how they can generate combat power for the JFC. Together, along with the course recommendations, provides a road map on how to

---

[54] Andrew Whitaker, Keatron Evans, and Jack B. Voth, *Chained Exploits: Advanced Hacking Attacks from Start to Finish* (Boston: Pearson Education, Inc., 2009), xvii.

[55] The SANS Institute is a cooperative research and education organization that provides security professionals, auditors, system administrators, and network administrators a venue to share lessons learned. See http://www.sans.org/about/sans.php for more information.

incorporate graduate-level academics into a joint professional military education program by following a building block approach.

CONCLUSION

Leveraging the electromagnetic spectrum will create an asymmetric advantage against adversaries in future conflicts. This can be accomplished through controlling the EMS, in a window of time and space, to provide an operational opportunity where none previously existed. The capabilities of computer network attack, electronic attack, electronic warfare support, and space control negation can produce effects that are just as tangible as GPS guided munitions. EMS control should not focus solely on causing destruction, but it instead, should identify methods to influence, disrupt, corrupt, and usurp the adversary's decision-making capacity.

Non-kinetic options must be employed in a *deliberate* manner to increase the enemy's observe, orient, decide, and act decision cycle. A physical region could be isolated, thus vulnerable, by neutralizing factor logical nodes within the network. The synchronization of target effects, discussed in section 2, illustrate notional vulnerabilities within an IADS. The way it receives, transmits, and processes data reveal themselves as decisive points. If the data is disrupted or corrupted, the system will present an inaccurate schema to human decision makers. Having a degraded OODA cycle, even for a finite slice of time, presents new options for meeting JFC objectives.

This scenario does not translate into "non-kinetics effects will always support kinetic operations." They *can* support kinetic fires, but it is not always the case. For example, a microwave relay tower or a fiber optic junction that eludes exploitation might become a target nominated for physical destruction that opens a non-kinetic attack vector. Once access is gained, the payload could be a computer network attack that neutralizes a now vulnerable industrial control system. Neutralizing this target, in a surgical manner, could be the effect that satisfies a JFC objective with minimal collateral damage.

In this regard, non-kinetic operations are just as complicated, if not more so, than conventional operations. A new team, with unique skill sets, is required to plan and coordinate these operations. Consolidating electronic attack, electronic warfare support, CNA, and space control under an NKDO for planning and execution provides the CFACC with tangible options that deliver combat power. These options further the joint campaign plan. Electronic warfare and computer network operations require the same level of command and control, integration, and synchronization as kinetic fires in order to produce discernible effects on the battlespace.

Final Thoughts

This monograph has shown the importance of non-kinetic operations in the generation of force to create a continued advantage. Its key strength is that the mechanism suggested to produce this combat power is not through the procurement of a technological solution, but through the cultivation of existing constructs and the expansion of the human cognitive dimension. Modifying current air operations center structures to accommodate the integration and synchronization of non-kinetic operations would benefit the entire joint force. Expanding the cognitive dimension requires a baseline of non-kinetic thought and intense training and academic programs to make non-kinetic operations a success.

The framework for negating an adversary's anti-access, area denial asymmetric advantage is through integrating non-kinetic operations to induce strategic paralysis within the enemy's decision cycle. Boyd calls this the mental-moral-physical being of an enemy. With regard to operational art, the fog and friction induced by non-kinetic operations increases the confusion within the enemy's decision cycle. With this in mind, can a non-kinetic force truly exist in warfare? Clausewitz's notion of force requires an evolution beyond its implied physical manifestation. The application of force is also through the asymmetrical apportionment of non-kinetic combat power to gain a localized advantage that collapses the adversary's means to resist. A new, holistic vision of force—attack-in-depth— must include the integration of kinetic and

non-kinetic combat power. This new idea of force generates options for the commander that increases advantage relative to that of the adversary.

UNCLASSIFIED

Overview

- Assumptions
- Networks
- Targeting
- Non-kinetic Effects Integration
- Non-kinetic Operations Package Commander
- Summary

UNCLASSIFIED

Assumptions

- Non-kinetic Effects (NKE)
  - Airborne EA (Radar / Communications)
  - Airborne ES
  - Network Warfare Operations (CNA/CNE)
  - Space Control Negation (Counter Communications)
- Tactical level of execution

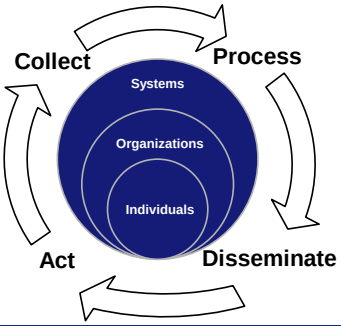
UNCLASSIFIED

Background

- Defining the EMS
  - The electromagnetic spectrum serves as the medium for the movement of data and information across all domains. (21CEW)
- What is EW?
  - Electronic warfare is defined as any action involving the use of the electromagnetic energy to control the EMS. (JP 13-1.1)
- How does IO fit?
  - The effects of IO are to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02 derived)

UNCLASSIFIED

Information Environment



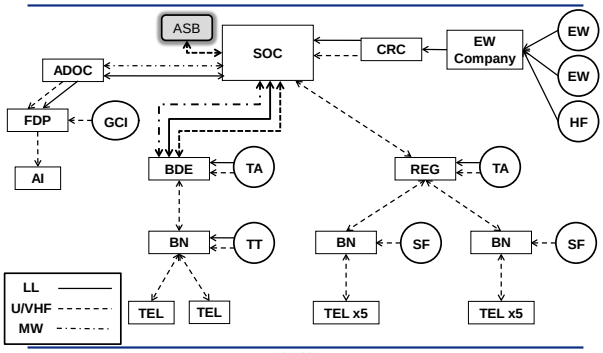
UNCLASSIFIED

Battlefield Networks

- Command, Control, Communications Systems (C3)
  - Proforma (Datalinks)
    - Air Surveillance
    - Battle Management
    - Weapons Control
  - Closed

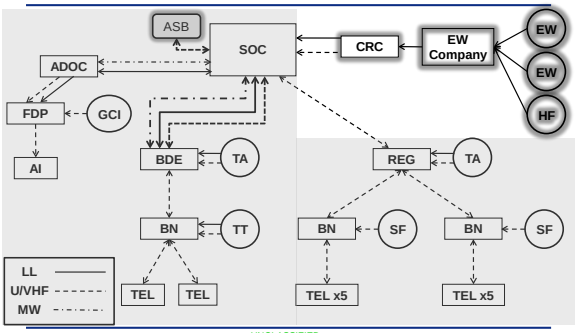
UNCLASSIFIED

Battlefield Networks



UNCLASSIFIED

Air Surveillance



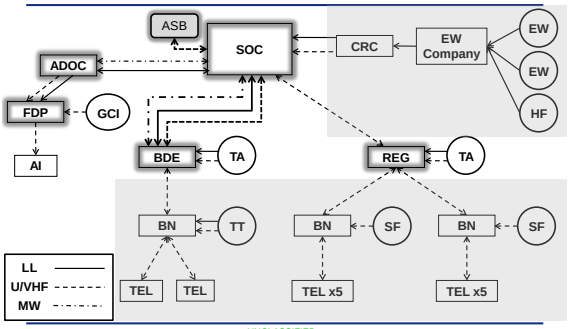
UNCLASSIFIED

Humble • Approachable • Credible

7

UNCLASSIFIED

Battle Management



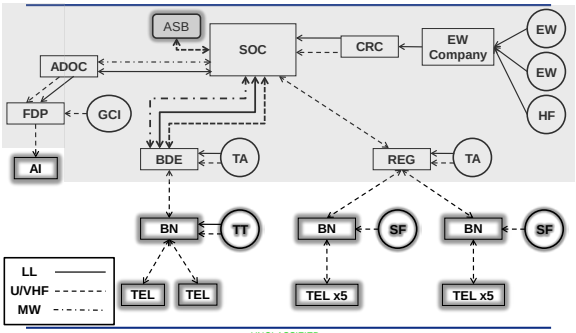
UNCLASSIFIED

Humble • Approachable • Credible

8

UNCLASSIFIED

Weapons Control



UNCLASSIFIED

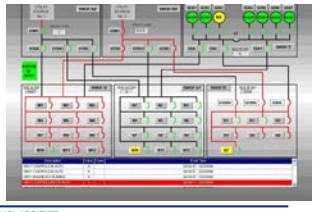
Humble • Approachable • Credible

9

UNCLASSIFIED

Industrial Control Systems

- Supervisory Control and Data Acquisition (SCADA)
  - Industrial processes (water / power generation)
  - Facility processes (mass transportation / HVAC)



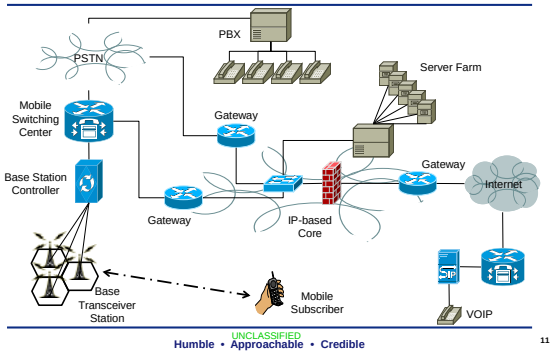
UNCLASSIFIED

Humble • Approachable • Credible

10

UNCLASSIFIED

Telecom Networks



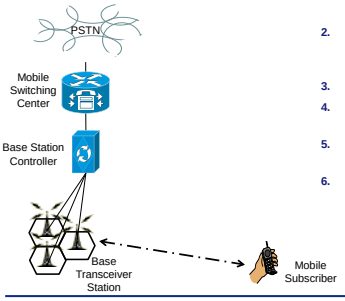
UNCLASSIFIED

Humble • Approachable • Credible

11

UNCLASSIFIED

Cellular (GSM)



1. Phone registers w/the network
2. Phone sends IMSI, IMEI, and GPS coords (if available) to BTS on control channel
3. BTS forwards data to MSC
4. MSC verifies user, assigns talk channels and TMSI
5. BTS forwards channels and TMSI to phone
6. Phone initiates call on assigned up/down link channels

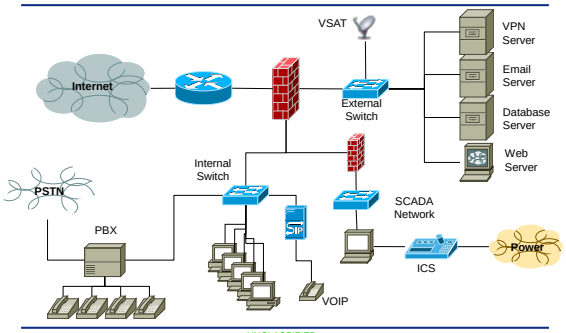
UNCLASSIFIED

Humble • Approachable • Credible

12

UNCLASSIFIED

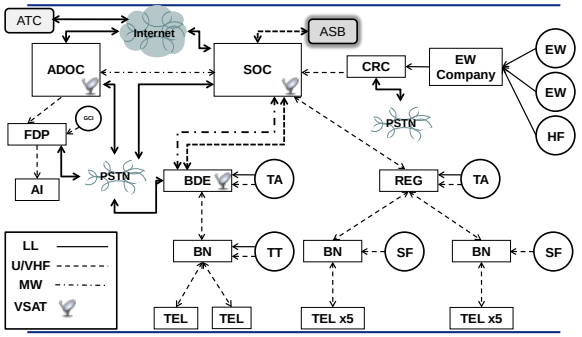
Local Area Network



UNCLASSIFIED
Humble • Approachable • Credible
15

UNCLASSIFIED

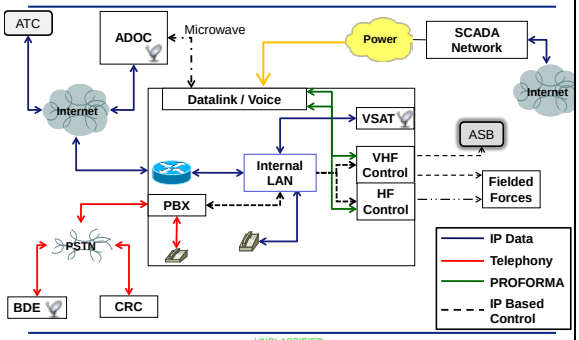
Threat Laydown



UNCLASSIFIED
Humble • Approachable • Credible
16

UNCLASSIFIED

Sector Operations Center

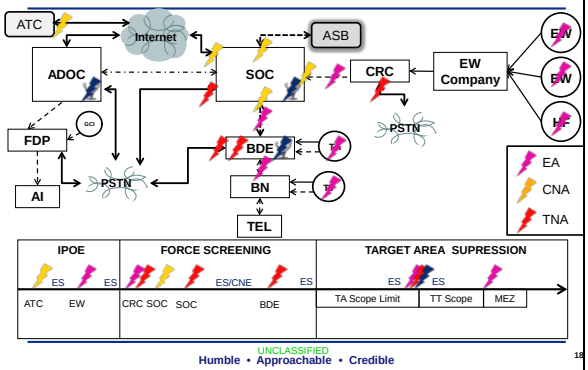


UNCLASSIFIED
Humble • Approachable • Credible
17

UNCLASSIFIED

Synchronized Effects

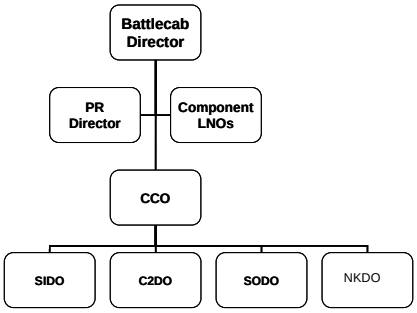
Objectives
1. Degrade EW
2. Isolate SOC
3. Deny Engagement



UNCLASSIFIED
Humble • Approachable • Credible
18

UNCLASSIFIED

NK Duty Officer



UNCLASSIFIED
Humble • Approachable • Credible
19

UNCLASSIFIED

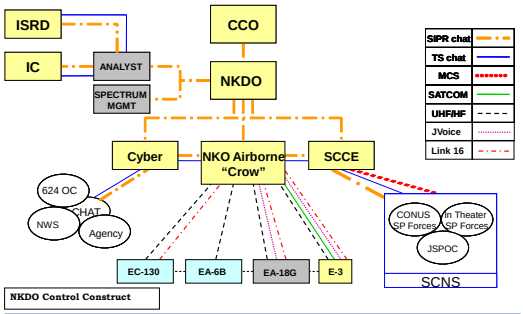
NK Duty Officer

- **Coordinate employment of all NKE in the ATO**
- **Monitors, coordinates, directs employment of all approved NKE assigned to support operations**
- **Recognize, recommend, and coordinate required effects to support *dynamic* and *emerging* target situations**
- **As required, coordination with tactical C2 to pass mission critical information to relevant package commanders**

UNCLASSIFIED
Humble • Approachable • Credible
20

UNCLASSIFIED

NK Duty Officer



UNCLASSIFIED

NKO Package Commander

- NKO Pkg/CC
  - Planning
    - Establish plans and contracts
    - Assign responsibilities
  - Execution
    - Maintain situation awareness on the battlespace
    - Decide on adjustments to current effects
    - Direct effects from appropriate asset

BIBLIOGRAPHY

Air Force Doctrine Document 3-1, Air Warfare. United States Air Force Chief of Staff, 2000.

Air Force Doctrine Document 3-12,Cyberspace Operations. United States Air Force Chief of Staff, 2011.

AFTTP 3-3.AOC, NKDO Team Section, Draft. US Air Warfare Center, 2011.

Andress, Jason. *The Basics of Information Security.* Waltham MA: Syngress Press, 2011.

Bailey, David, and Wright, Edwin. *Practical SCADA for Industry*. IDC Technologies, 2003.

Bartlett, F.C. *Remembering: An Experimental and Social Study*. Cambridge: Cambridge University Press, 1932.

Bousquet, Antoine. *The Scientific Way of Warfare*. New York, NY: Columbia University Press, 2009.

Boyd, John. *Destruction and Creation*, unpublished essay, 1976.

Boyd, John. *Patterns of Conflict*, unpublished presentation, draft version, 1982.

Boyd, John. *Organic Design for Command and Control*, unpublished presentation, 1987.

Campaign Planning Handbook. United States Army War College Department of Military Strategy, Planning, and Operations Carlisle Barracks, Pennsylvania, 2012.

CIA Historical Review Program. *Air Defense of the USSR, release as sanitized*. US Central Intelligence Agency, 1999.

Clausewitz, Carl von. *On War. Ed. and trans. Howard, Michael and Peter Paret*. Princeton, NJ: Princeton University Press, 1976.

Darley, William M. "Clausewitz's Theory of War and Information Operations." *Joint Force Quarterly* 1st Quarter, no. 40 (2006): 73-79.

D'Amura, Ronald M. "Campaigns: The Essence of Operational Warfare." *Parameters* (US Army War College) 17, no. 2 (Summer 1987): 42-51.

de Czege, Huba Wass. "Systemic Operational Design: Learning and Adapting in Complex Missions." *Military Review* (January–February 2009): 2-13.

Dickson, Keith D. "Operational Design: A Methodology for Planners." *Journal of the Department of Operational Art and Campaigning*, Joint Advanced Warfighting School (Spring 2007): 23–38.

Dolman, Everett C. *Pure Strategy*. New York: Frank Cass, 2005.

Duggan, David, et al., *Penetration Testing of Industrial Control Systems*, Sandia National

Laboratories, 2005.

Evans, Michael. "Centre of Gravity Analysis in Joint Military Planning and Design: Implications and Recommendations for the Australian Defense Force." *Security Challenges*, vol 8, No. 2 (Winter 2012): pp 81-104.

Elder, Robert J., Lt Gen, USAF (Ret). *21st Century Electronic Warfare*. Association of Old Crows, 2010.

Frazer, Roy. *Process Measurement and Control – Introduction to Sensors, Communication Adjustment, and Control*, Prentice-Hall, Inc., 2001.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International, 1964.

Graham, Adrian W. *Communications, Radar, and Electronic Warfare*. Wiley, 2011.

Greene, Robert. *The 33 Strategies of War*. New York: Penguin, 2007.

Halpern, Jason. *IP Telephony Security in Depth*. Cisco Systems, 2003.

Howard, Dr. Ronald A. "Speaking of Decisions: Precise Decision Language." *Decision Analysis* 1, no. 2 (June 2004).

Idaho National Laboratory, *Control Systems Cyber Security: Defense in Depth Strategies.* Homeland Security, May 2006.

ISA-TR99.03.01: *Security Technologies for Industrial Automation and Control Systems*. ISA, 2007.

Jabbour, Kamal T., Dr. *50 Cyber Questions Every Airman Can Answer*. Air Force Research Laboratory, 2008.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. Joint Chiefs of Staff, 2011.

Joint Publication 3-01, Countering Air Missile Threats. Joint Chiefs of Staff, 2007.

Joint Publication 3-13, Information Operations. Joint Chiefs of Staff, 2012.

Joint Publication 3-30, Command and Control for Joint Air Operations. Joint Chiefs of Staff, 2010.

Joint Publication 5-0, Joint Operations Planning. Joint Chiefs of Staff, 2011.

Kem, Jack D. *Campaign Planning: Tools of the Trade*. 2nd ed. Fort Leavenworth, KS: Department of Joint and Multinational Operations, US Army Command and General Staff College, June 2006.

Kopp, Carlo, Dr. SAM *System Mobility: Russian and PLA Air Defense System Vehicles*. Technical Report APA-TR-2008-0601. Air Power Australia, 2012.

Kuhn, Thomas S. *The Structure of Scientific Revolutions, 3rd Edition*. Chicago: The University of Chicago Press, 1996.

Mintz, Alex. "How Do Leaders Make Decisions?: A Polyheuristic Perspective." *Journal of Conflict Resolution* 48, no. 1 (1 February 2004): 30-13.

Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Operational Theory*. Portland, OR: Frank Cass, 1997.

Orange, Marc and Turner, Brough. *3G Tutorial*. NMS Communications, 2002.

Osinga, Frans. *Science, Strategy, and War: The Strategic Theory of John Boyd*. New York, NY: Routledge, 2007.

Paiget, J., & Inhelder, B. *Memory and Intelligence*. London: Routledge and Kegan Paul, 1973.

Qiao, Liang, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999.

Reilly, Jeffrey M., Dr,. *Operational Design: Distilling Clarity from Complexity for Decisive Action*. Air University Press, 2012.

Stouffer, Keith and Falco, Joe and Scarfone, Karen. *Guide to Industrial Control Systems Security*. US Department of Commerce: National Institute of Standards and Technology, June 2011.

Strange, Joseph. "Centers of Gravity and Critical Vulnerabilities: Building on the Clausewitzian Foundation So We Can All Speak the Same Language." *Perspectives on Warfighting Series*, no. 4, 2nd ed. (1996).

Tol, Jan van, with Gunzinger, Mark and Krepinevich, and Thomas, Jim. *AirSea Battle: A Point-of-Departure Operational Concept*. Washington D.C.: Center for strategic and budgetary assessments, 2010.

Training and Doctrine Command (TRADOC) Pamphlet 5255500. *Commander's Appreciation and Campaign Design*. version 1.0, 28 January 2008.

Whitaker, Andrew, Keatron Evans, and Jack B. Voth. *Chained Exploits: Advanced Hacking Attacks from Start to Finish*. Boston: Pearson Education, Inc., 2009.